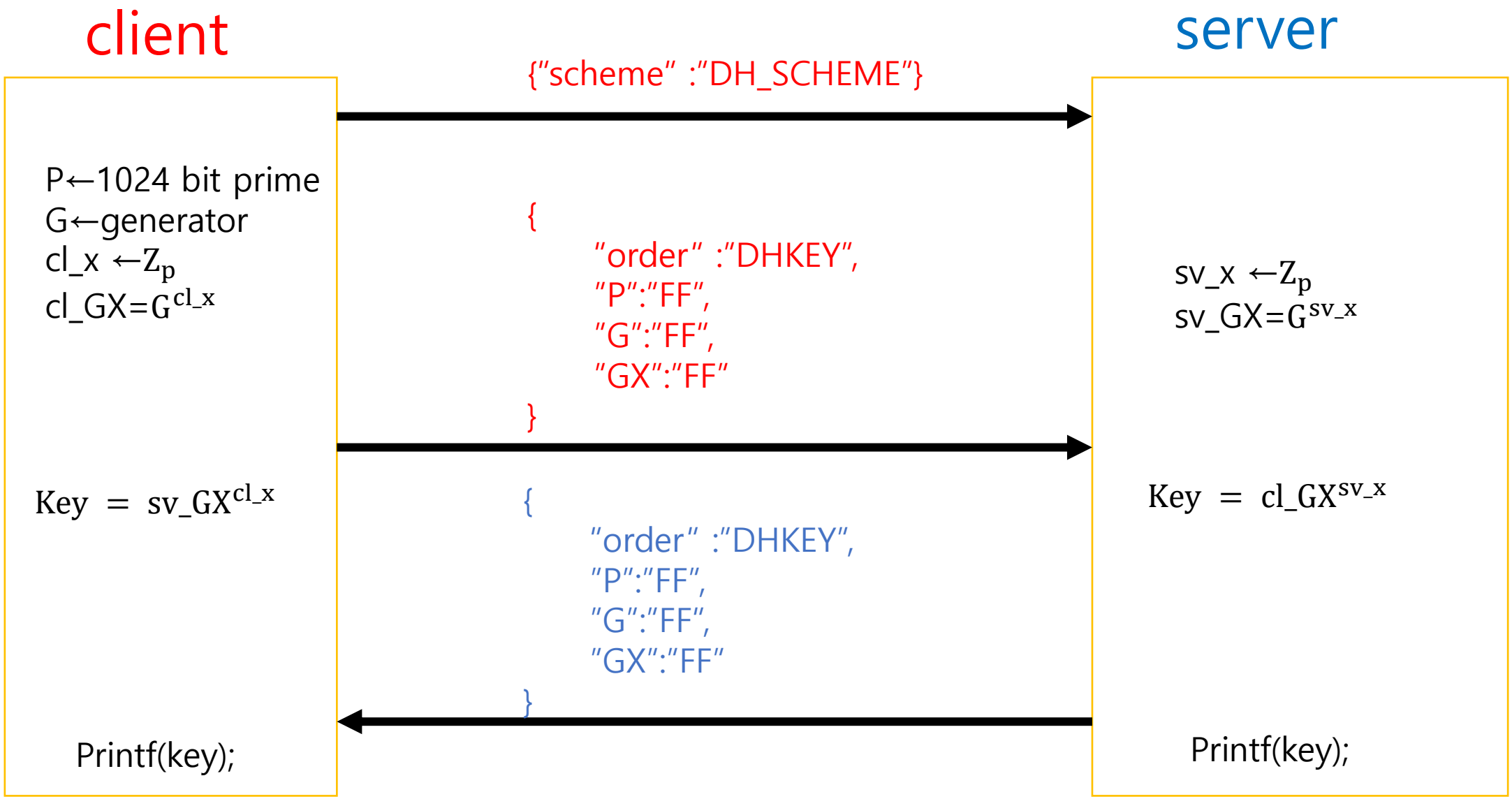
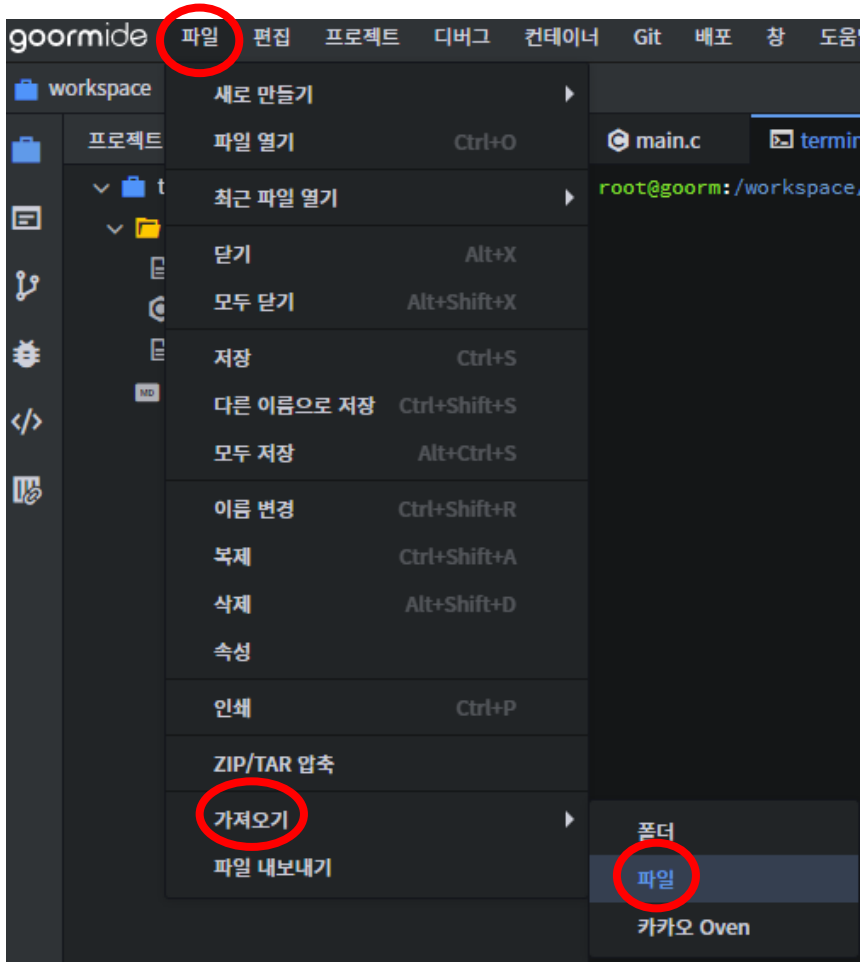
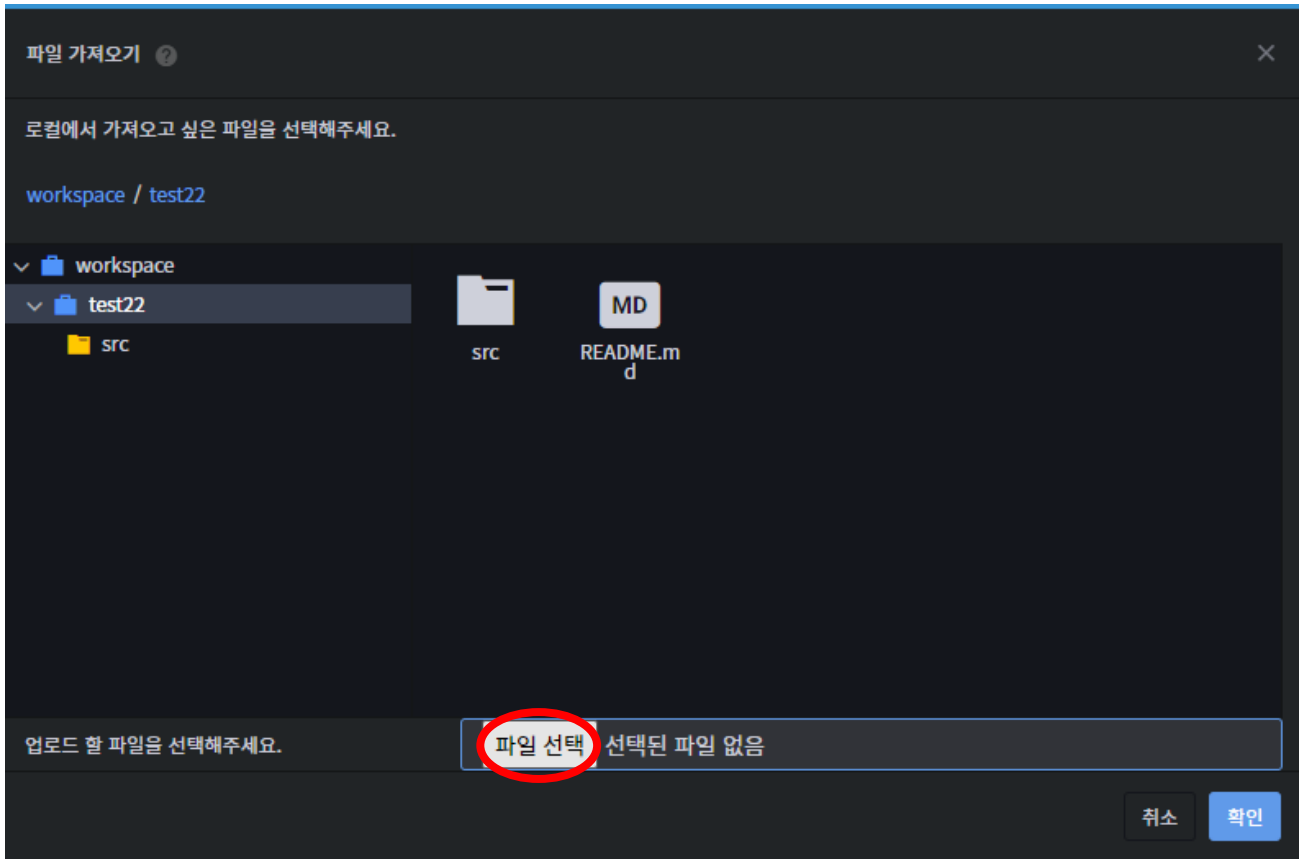
DH key Exchange 과제

HOMEWORK


client
server
{"scheme" :"DH_SCHEME"}
P←1024 bit prime
G←generator
cl_x ←Z_p
cl_GX=G^{cl_x}
{
"order" :"DHKEY",
"P":"FF",
"G":"FF",
"GX":"FF"
}
sv_x ←Z_p
sv_GX=G^{sv_x}
Key = $sv\_GX^{cl\_x}$
{
"order" :"DHKEY",
"P":"FF",
"G":"FF",
"GX":"FF"
}
Key = $cl\_GX^{sv\_x}$
Printf(key);
Printf(key);

서버 사용법





다운받은 server 파일 선택 후 확인

서버 사용법

server 파일 위치로 이동 후

./server [PORT]

Default PORT: 29090 // PORT 지정 않는 경우 **(./server)**

포트포워딩 + 추가

유형	내부 포트	IP	외부 포트	명령어
SSH	22	54.180.153.213	53180	ssh -p 53180 root@54.180.153.213
사용자 지정	29090	54.180.153.213	50213	54.180.153.213:50213
사용자 지정	13597	54.180.153.213	58386	54.180.153.213:58386

SSH/포트포워딩 기능은 컨테이너가 동작 중일 때 사용할 수 있습니다.

서버 실행 (클라이언트 대기 상태)

```
root@goorm:/workspace/Programming/src/4lcrypto# ./server
===[PORT] : 29090====
Server waiting connection request
```

클라이언트 실행

```
root@goorm:/workspace/Programming/src# gcc -o test test.c -lssl -lcrypto -ljson-c
root@goorm:/workspace/Programming/src# ./test 54.180.153.213 50213
```

클라이언트와 통신이 끝나면 서버는 사용자 입력을 대기합니다.
이 때 s 키를 누르면 다시 시작하고 (새로운 client가 connect 할 때까지 대기상태),
f를 누르면 서버를 안전하게 종료하게 됩니다.
단, connect 대기 상태일때는 키 입력을 받지 않으므로 안전한 종료를 위해서 반드시 client 프로그램이 한번 다 돌아간 뒤에 f키를 눌러서 종료해주세요.

※서버 강제종료는 Ctrl + c, “Server can not bind local address” 에러 발생 할 수도 있음

※주의사항

1.
Server 실행파일을 다운받은 후 실행을 했을 때
bash: ./server: 허가 거부　　란 오류 메세지가 뜬다면
chmod 777 server　명령어를 쳐주세요.

2.
Key값이 다를 경우 간단한 오류 메세지를 출력해줍니다.
예) key값에 scheme이 없을 경우
ERROR KEY scheme
JSON KEY ERROR

3.
포트가 bind 될 경우가 생기는데, 그럴 경우엔
새로운 포트번호(큰 번호로)를 추가하시거나,
(기존의 66번 포트는 안됩니다.)
또는 일정시간 기다리시면 됩니다.
"Server can not bind local address"

4.
내부 포트번호는 바뀌지 않지만 외부 포트번호와 IP는 변동될 수 있으니 실행이 안될 경우 확인해주세요.

출력 예

- 클라이언트

```
root@goorm:/workspace/test22/src# ./test 3.36.68.152 51883
sended : { "scheme": "DH_SCHEME" }
sended : { "order": "DHKEY", "P": "FF31EE6607BBBD5F978FDB99450DA56381FBC8189A966A0B6083DA6D8C926F455546D41CF41AB609235C953C0F17CD44EFE7B1EDD594F588F7EED820024C435C91EC30A8FA24804193292AF3DF0431C36F473DEAE8A6D4146DD9466C5B6ED98A3B83
37EB9AB73FF55C7345FAA601D6303383F9EA1CB8A4E29F1ED074ED51EDB7", "G": "05", "GX": "D92825A0A6AA5361E84EC850FC1ECBB204773812398B1FBDEC11BE322F9E2596146A3E480B94185F7C6206662C3CB09726680DD245F892B1A02F99B3DE6682C09F601F2DD3E12E1E41218C
49B6DBEBAB7091996C93E16A110A76D09D493DA38913809F2AD47837C610797AFEB49000E4993C26C3F82B96E65101277F75F753BF" }
received data : { "order": "DHKEY", "P": "FF31EE6607BBBD5F978FDB99450DA56381FBC8189A966A0B6083DA6D8C926F455546D41CF41AB609235C953C0F17CD44EFE7B1EDD594F588F7EED820024C435C91EC30A8FA24804193292AF3DF0431C36F473DEAE8A6D4146DD9466C5B6ED
98A3B8337EB9AB73FF55C7345FAA601D6303383F9EA1CB8A4E29F1ED074ED51EDB7", "G": "05", "GX": "5A442CB440F0911EC72D37494C6462B33B9CC86C6248B3A8C5B24F2500AA2908DC5F8FAFE2123B38F804764E460AF4C7359F6C7C579845BA402C52B112B323FD6D61F0094D91EB5
AB219370A4B1FDB9A4B4F30CF45DA17DC9F7B7F94768B02F3FF4F192177CDA4CD89C12FF3C3FF44249855FB9D723B72560730DF25119773CF" }
DH key exchange result : BEB8A920C2776CEC242E1C3D9E451AA689EA0B66565BC4D8F4F3AFDB679D9E30787B1972A94E89228A8D6DD883F6F623C2217D64F6421D4CF34A2BF4D25333DAAD0D1FB3724BD1F1BDFF5C64C076A08E3B5143D0DCA70EF6EBEDD15B1D4C9C702B8E4CA18712E
7F1101B27ED88C3E20CB45969012B133535573A97B6EA18102
```

- 서버

```
root@goorm:/workspace/test22/src# ./server
===[PORT] : 29090=====
Server waiting connection request
3.36.68.152 client connect

3.36.68.152(42202) entered
recv data : { "scheme": "DH_SCHEME" }
recv data : { "scheme": "DH_SCHEME" }
sended : { "order": "DHKEY", "P": "FF31EE6607BBBD5F978FDB99450DA56381FBC8189A966A0B6083DA6D8C926F455546D41CF41AB609235C953C0F17CD44EFE7B1EDD594F588F7EED820024C435C91EC30A8FA24804193292AF3DF0431C36F47
3DEAE8A6D4146DD9466C5B6ED98A3B8337EB9AB73FF55C7345FAA601D6303383F9EA1CB8A4E29F1ED074ED51EDB7", "G": "05", "GX": "5A442CB440F0911EC72D37494C6462B33B9CC86C6248B3A8C5B24F2500AA2908DC5F8FAFE2123B38F80476
4F460AF4C7359F6C7C579845BA402C52B112B323FD6D61F0094D91EB5AB219370A4B1FDB9A4B4F30CF45DA17DC9F7B7F94768B02F3FF4F192177CDA4CD89C12FF3C3FF44249855FB9D723B72560730DF25119773CF" }
DH key exchange result : BEB8A920C2776CEC242E1C3D9E451AA689EA0B66565BC4D8F4F3AFDB679D9E30787B1972A94E89228A8D6DD883F6F623C2217D64F6421D4CF34A2BF4D25333DAAD0D1FB3724BD1F1BDFF5C64C076A08E3B5143D0DCA70E
F6EBEDD15B1D4C9C702B8E4CA18712E77F1101B27ED88C3E20CB45969012B133535573A97B6EA18102
```

※DH KEY가 같은 지 확인